VU VRIJE UNIVERSITEIT AMSTERDAM

VU Research Portal

How to Keep Your Memory Safe and Your Software Fast

Kroes, T.

2020

document version
Publisher's PDF, also known as Version of record

Link to publication in VU Research Portal

citation for published version (APA)
Kroes, T. (2020). *How to Keep Your Memory Safe and Your Software Fast*. [PhD-Thesis - Research and graduation internal, Vrije Universiteit Amsterdam].

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:
vuresearchportal.ub@vu.nl

Download date: 04. May. 2023

VRIJE UNIVERSITEIT

HOW TO KEEP YOUR MEMORY SAFE AND YOUR SOFTWARE FAST

PH.D. THESIS

Taddeüs Kroes

The research reported in this dissertation was conducted at the Faculty of Science, at the Department of Computer Science, of the Vrije Universiteit Amsterdam.

This work is part of the research programme *Vici* with project number 639.023.309 titled “Dowsing”, which is funded by the Dutch Research Council (NWO).

Copyright © 2020 by Taddeüs Kroes

Cover and chapter illustrations by Mei-Li Nieuwland

VRIJE UNIVERSITEIT

HOW TO KEEP YOUR MEMORY SAFE AND YOUR SOFTWARE FAST

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad Doctor of Philosophy
aan de Vrije Universiteit Amsterdam,
op gezag van de rector magnificus
prof.dr. V. Subramaniam,
in het openbaar te verdedigen
ten overstaan van de promotiecommissie
van de Faculteit der Bètawetenschappen
op maandag 28 september 2020 om 15.45 uur
in de aula van de universiteit,
De Boelelaan 1105

door

Taddeus Kroes

geboren te Amsterdam

promotor: prof.dr.ir. H.J. Bos
copromotor: dr. C. Giuffrida

"This will be a very short project, I promise."

Cristiano Giuffrida, in 2016, 2017, 2018 and 2019.

Acknowledgements

Even though doing a Ph.D. is often a lonely journey, at the end of it I have many people to thank for being there along the way.

First, I want to thank Herbert Bos for being an amazing supervisor. You gave me complete freedom in pursuing my own projects, and empowered me to conduct research with pride and integrity. Even when I lost all motivation after a sea of negative reviews for some projects, you convinced me the work I did was "just super cool". I am grateful to have been exposed to that energy.

I am equally grateful for the energy of my copromotor, Cristiano Giuffrida. You are the most creative researcher I could imagine, always coming up with cool new ideas. I will miss our conversations that, while they always took at least twice the allocated time, never failed to leave me knowing exactly what to do next.

Next, I sincerely thank the members of my thesis committee: Stefan Bunthaler, Cristian Cadar, Thorsten Holz, Alex Iosup, and Asia Slowinska. Thank you all for dedicating your time to reviewing my work, and for helping me improve it.

During my research, I was fortunate enough to collaborate with some great people. In fact, I share first authorship on several chapters of this dissertation. Special thanks go to Koen Koning. We started off working on Delta Pointers together, but also after that you helped me out countless times in work you were not even involved in. But more importantly, you have been a good friend all throughout. Erik, thank you for involving me in the Type-After-Type paper and for making it a notably smooth co-working experience. Anil and Joseph, thank you for continuing my work on BinRec all the way up in Irvine, California. Many thanks to all the students and postdocs there who helped publish the work after such a long struggle.

In addition to the colleagues I collaborated with directly, I will never forget working alongside so many smart people at VUSec. Thanks to my roomie Lucian for all our conversations and friendship. To István, for teaching me how binaries work. To Alyssa for being a smart and sensible sounding board. To Kaveh for the laughs. To all the others for some great borrels and chats: Andrea, Andrei (both of them), Angelos, Ben, Brian, Dennis, Elia, Emanuele, Enes, Erik B., Hany, Kousthuba, Manolis, Manuel (get Vim!), Marco, Marius (thanks for the thesis pass!), Michael, Natalie, Pietro, Radhesh, Sanjay, Sebastian, Stephan, and Vic-

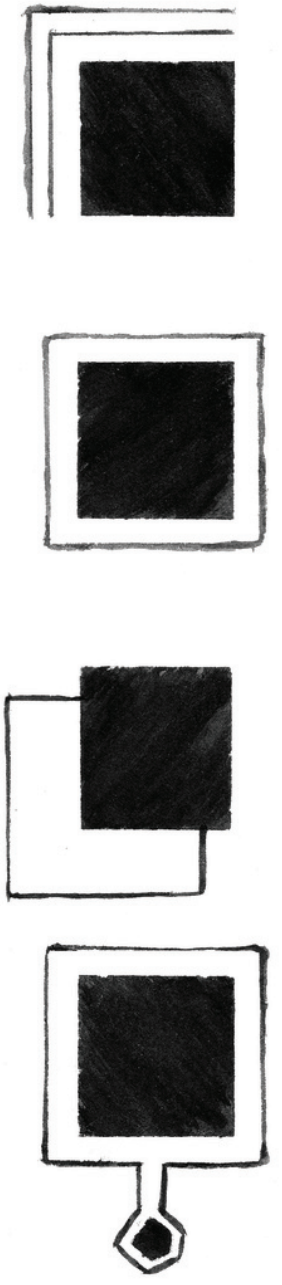
tor. Thank you all! And of course, thank you Caroline and Mojca for ever so swiftly taking care of the administrative “rompslomp”.

In the last year of my Ph.D., I went on an internship at Google in New York. Although that has little to do with this thesis directly, I view my experience there as part of my Ph.D. journey and would like to take this opportunity to thank the people involved in making it an awesome one. László and Wei, thank you for supervising me and giving me so much freedom in my work. Stefan, I am happy to have gained you as a friend, and grateful for your professional guidance. Markus, thanks for showing me all the cool lunch spots! Franjo, thank you for showing me that managers can actually be a great influence.

Besides all the people I met at work, there are just as many people to thank for keeping me sane in my personal life. Rowan, buddy, thanks for being there during the lows and the highs. For all the long gaming sessions in which I could vent. For the meaningful talks, but especially the meaningless ones. Raphael, you are an excellent person and friend. I cherish our conversations and the way they have helped me grow. Stijn, I enjoyed our frequent Friday night beers & laughs about academia. Ger and Renate, thanks for all the board game nights! To Richard, Sander, Jayke, Gijs, Rik, and all my other nerd friends: I’m looking forward to our next Corona-free borrel! Simon, our bike rides have been a great way to convert all kinds of energy into a positive kind. Let’s keep them coming. To my parents and numerous siblings: thank you for always supporting my choices.

Mei-Li, words cannot describe how lucky and grateful I feel to have you in my life. You have made me a more complete person. Thank you for supporting me. Thank you for being you. I also love that we got to work together sometimes. Or, rather, you working hard to make computer science look as cool as it can be. You made everything from conference posters, to course mascots, to the beautiful illustrations in this thesis(!) Thank you for letting me share my work with you in that way, it means the world to me.

Taddeüs Kroes
Amsterdam, The Netherlands, August 2020



Contents

List of Figures

List of Tables

List of Listings

Publications

This dissertation includes several research papers, as appeared in the following conference proceedings. The text differs from the published versions in minor editorial changes made to improve readability, and added clarifications to address comments by the committee:

Taddeus Kroes[1], Koen Koning[1], Erik van der Kouwe, Herbert Bos, and Cristiano Giuffrida. **Delta Pointers: Buffer Overflow Checks Without the Checks.** In *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18)*, page 22. April 23-26, 2018, Porto, Portugal.
[Appears in Chapter 2]

Taddeus Kroes, Chris Ouwehand, Cristiano Giuffrida, and Herbert Bos. **RedPool: Slabifying Redzones for Efficient Spatial Memory Safety.** *Under review*
[Appears in Chapter 3]

Erik van der Kouwe, Taddeus Kroes, Chris Ouwehand, Herbert Bos, and Cristiano Giuffrida. **Type-After-Type: Practical and Complete Type-Safe Memory Reuse.** In *Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC '18)*, pages 17–27. December 3-7, 2018, San Juan, Puerto Rico.
[Appears in Chapter 4]

Anil Altinay[1], Joseph Nash[1], Taddeus Kroes[1], Prabhu Rajasekaran, Dixin Zhou, Adrian Dabrowski, David Gens, Yeoul Na, Stijn Volckaert, Cristiano Giuffrida, Herbert Bos, and Michael Franz. **BinRec: Dynamic Binary Lifting and Recompilation.** In *Proceedings of the Fifteenth EuroSys Conference (EuroSys '20)*, pages 1–16. April 27-30, 2020, online virtual conference.
[Appears in Chapter 5]

[1]Equal contribution shared first authors.

Related publications not included in the dissertation are listed in the following:

Taddeus Kroes[1], Koen Koning[1], Cristiano Giuffrida, Herbert Bos, and Erik van der Kouwe. **Fast and Generic Metadata Management with Mid-Fat Pointers.** In *Proceedings of the 10th European Workshop on Systems Security (EuroSec '17)*. April 23, 2017, Belgrade, Serbia.

Taddeus Kroes[1], Anil Altinay[1], Joseph Nash[1], Yeoul Na, Stijn Volckaert, Herbert Bos, Michael Franz, and Cristiano Giuffrida. **BinRec: Attack Surface Reduction Through Dynamic Binary Recovery.** In *Proceedings of the 2018 Workshop on Forming an Ecosystem Around Software Transformation (FEAST '18)*, pages 8–13. November 15, 2019, Toronto, Canada.

Publications not related to this dissertation, but published in refereed conferences are listed in the following:

Lucian Cojocar, Taddeus Kroes, and Herbert Bos. **JTR: A Binary Solution for Switch-Case Recovery.** In *Proceedings of the International Symposium on Engineering Secure Software and Systems 2017 (ESSoS '17)*. July 4-5, 2017, Bonn, Germany.

[1]Equal contribution shared first authors.